UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------x
UNITED STATES OF AMERICA,

- against -

ADIS MEDUNJANIN,

Defendant.
----------x

MEMORANDUM OF DECISION

10 CR 19 1 (RJD)

DEARIE, District Judge.

Defendant Adis Medunjanin awaits trial on charges that he conspired with Najibullah Zazi and others to commit coordinated bombings within the New York City subway system on behalf of al-Qaeda. In a successful effort to derail what was believed to be an imminent terrorist attack, federal and state agents physically searched the residences and otherwise monitored the activities and communications of defendant, his alleged co-conspirators and others potentially involved in or aiding and abetting the plot.

On January 19, 2010, as required by 50 U.S.C. §§ 1806(c) and 1825(d), the government notified defendant of its intent to introduce at trial evidence obtained pursuant to the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 et seq. See ECF Docket # 82, Exhibit A, Notice. This notice confirms both that the Attorney General authorized disclosure of the evidence in a criminal proceeding, see 50 U.S.C. § 1806(b), and that defendant is an "aggrieved person"[1] with standing to challenge the legality of the subject surveillance, see 50 U.S.C. §§ 1806(c) & 1825(d) (requiring prior notice if the United States intends to introduce or disclose FISA-acquired evidence "against an aggrieved person" during a trial or other proceeding).

[1] FISA defines an "aggrieved person" both as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance," 50 U.S.C. § 1801(k), and as "a person whose premises, property, information, or material is the target of physical search or any other person whose premises, property, information, or material was subject to physical search," 50 U.S.C. § 1821(2).

On February 11, 2011, defendant moved to suppress all FISA-derived evidence "on the ground[] that [it] was unlawfully acquired."[2] 50 U.S.C. § 1806(e)(1). In the alternative, defense counsel requested access to the FISA applications and orders (also known as "dockets") in as much as it was "necessary" to aid the Court in "mak[ing] an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f). In response, the government offered a comprehensive classified submission refuting the defendant's arguments and appending, for in camera and ex parte review, the FISA dockets relating to the surveillance in question. On September 8, 2011, the Court denied defendant's FISA suppression motion. ECF Docket # 147. Although given the classified nature of the materials involved, the Court is "necessarily circumspect in [its] discussion," United States v. Abu-Jihaad, 630 F.3d 102, 130 (2d Cir. 2010), the rationale for that ruling follows.

I. DISCUSSION

A. Constitutionality of FISA

"Enacted in 1978, FISA permits the Chief Justice of the United States to designate eleven federal judges as the Foreign Intelligence Surveillance Court ("FISA Court") with jurisdiction to entertain ex parte executive applications for electronic surveillance for the purpose of obtaining foreign intelligence information."[3] Abu-Jihaad, 630 F.3d at 117 (internal quotation marks and citations omitted); see generally In re Sealed Case, 310 F.3d 717, 722-23 (FISA Ct. Rev. 2002). "Congress passed FISA to settle what it believed to be the unresolved question of the

[2] Some of the FISA-acquired evidence has already been disclosed and used offensively by the defense. The government unsealed and produced a number of FISA procured communications to and from defendant's lawyer after defendant referred to certain lawyer-client communications in support of his motion to suppress post-arrest statements made to law-enforcement agents. Defendant himself offered certain of these attorney-client communications during the hearing on the suppression motion.

[3] "Although FISA originally applied only to electronic surveillance, the law was amended in 1994 to extend to physical searches for foreign intelligence information." Abu-Jihaad, 630 F.3d at 117 n.18 (citing Pub. L. No. 103–359, 108 Stat. 3444 (1994)). The standards governing applications and orders for the two types of surveillance are similar, although not identical. Where appropriate, this opinion refers generally to the provisions governing electronic surveillance. The Court's affirmance of the legality of that surveillance extends to the legality of any physical searches that may have occurred pursuant to FISA.

applicability of the Fourth Amendment warrant requirement to electronic surveillance for foreign intelligence purposes, and to remove any doubt as to the lawfulness of such surveillance." United States v. Stewart, 590 F.3d 93, 126 (2d Cir. 2009) (internal quotation marks omitted). Accordingly, courts within the Second Circuit repeatedly have upheld the legality of FISA's provisions in light of the requirements imposed on the government in conducting surveillance to acquire foreign intelligence information in particular cases. See, e.g., United States v. Abu-Jihaad, 531 F.Supp.2d 299 (D. Conn. 2008), aff'd, 630 F.3d 102; United States v. Sattar, No. 02 CR. 395 JGK, 2003 WL 22137012 (S.D.N.Y. Sept. 15, 2003), aff'd sub nom. United States v. Stewart, 590 F.3d 93 (2d Cir. 2009); United States v. Rahman, 861 F.Supp. 247 (S.D.N.Y. 1994), aff'd, 189 F.3d 88 (2d Cir. 1999); United States v. Megahey, 553 F.Supp. 1180 (E.D.N.Y. 1982), aff'd sub nom. United States v. Duggan, 743 F.2d 59 (2d Cir. 1984). Nevertheless, for the express purpose of preserving the arguments for appeal, defendant urges this Court to declare FISA unconstitutional and to suppress the FISA-derived evidence the government intends to introduce at defendant's trial.[4] ECF Docket # 100, Exh. 3, Defense Brief ("Def. Br.") at 4. Most of defendant's arguments are foreclosed by controlling precedent, and the balance are unpersuasive.

1. Standard for Probable Cause

First, defendant argues that FISA violates the Fourth Amendment because it does not require a demonstration of probable cause to believe that the resulting surveillance will reveal foreign intelligence information.[5] Def. Br. at 5. While it is true that FISA does not require this

[4] The government outlines the sources of this information on pages 9-10 of its classified submission. Defendant is "aggrieved" by a subset of the surveillance, which this opinion addresses; no ruling is required for the remainder, which he lacks standing to challenge. See supra note 1.

[5] FISA defines "foreign intelligence information," see 50 U.S.C. § 1801(e), as:
(1) information that relates to, and if concerning a United States person is necessary to, the ability of the Unites States to protect against –
(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

particular probable cause demonstration, that fact is without constitutional consequence. "To issue a FISA warrant, a judge must find, inter alia, that there is probable cause to believe that the target of the surveillance is a 'foreign power or an agent of a foreign power' and that the place or facilities to be surveilled are 'being used, or . . . about to be used, by a foreign power or an agent of a foreign power.'" Abu-Jihaad, 630 F.3d at 117-18 (quoting 50 U.S.C. § 1805(a)(2)(B)) (emphasis added). "These requirements make it reasonable to dispense with a requirement that the FISA Judge find probable cause to believe that surveillance will in fact lead to the gathering of foreign intelligence information." Duggan, 743 F.3d at 73 ("[T]he procedures fashioned in FISA a[re] a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information.").

2. Purpose of Surveillance

Second, defendant submits that permitting FISA warrants upon a showing that a "significant purpose" of the surveillance is to obtain foreign intelligence information violates the Fourth Amendment. Def. Br. at 5. The Second Circuit recently rejected this precise argument in a comprehensive opinion examining the issue from every conceivable angle. See Abu-Jihaad, 630 F.3d at 131 ("[W]e identify no constitutional infirmity in Congress's decision to allow FISA warrants to issue on certification of a 'significant purpose' to obtain foreign intelligence information . . . ."); see id. at 128-29 ("[W]e hold that certification of a significant purpose to obtain foreign intelligence information, together with satisfaction of all other FISA requirements,

---

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to –
(A) the national defense or the security of the United States; or
(B) the conduct of the foreign affairs of the United States.
FISA defines a "foreign power," in part, as "a group engaged in international terrorism or activities in preparation therefor." 50 U.S.C. § 1801(a)(4).

is reasonable and, therefore, sufficient to support the issuance of a warrant under the Fourth Amendment.").

3. Minimization Procedures

Third, defendant contends that FISA's "open-ended and government-defined minimization procedures" render all surveillance unconstitutional, as does permitting the executive branch to define its own minimization standards, which the FISA Court then "rubber stamps." Def. Br. at 5-6. These arguments are unconvincing.

The FISA Court does not, as defendant asserts, capitulate to the executive's unilateral determinations regarding whether and how to minimize non-pertinent communications. Rather, FISA mandates the implementation of . . .

> . . . specific procedures, which shall be adopted by the Attorney General, that are *reasonably designed in light of the purpose and technique of the particular surveillance*, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. [6]

50 U.S.C. § 1801(h)(1) (emphasis added). The FISA Court thus has the power independently to assess whether the FISA "application properly proposes, as required by § 1801(h), to minimize the intrusion upon the target's privacy." Duggan, 743 F.2d at 73-74. Before approving or ratifying surveillance, the FISA Court must determine that the proposed minimization procedures fit the statutory definition—specifically, that they are reasonable "in light of the purpose and technique of the particular surveillance" requested. 50 U.S.C. § 1801(h)(1); see also 50 U.S.C. § 1805(a)(3) (a FISA Court judge "shall . . . approv[e] the electronic surveillance if he finds that, [inter alia,] . . . the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title.").

[6] "To fulfill that statutory duty, the Attorney General has adopted standard minimization procedures that apply to every FISA application, which were submitted to the Court for in camera review." Abu-Jihaad, 531 F.Supp.2d at 303 n.4.

Likewise, the minimization procedures necessarily are not "open-ended" by virtue of the requirement that they must be reduced to writing and submitted for judicial approval in every application, in every case. See 50 U.S.C. § 1804(a)(4) (requiring every FISA application to include a "statement of the proposed minimization procedures"); 50 U.S.C. § 1805(a)(3) (requiring a FISA Court to find that "the proposed minimization procedures meet the definition of minimization procedures under" FISA); id. § 1805(c)(2)(A) (requiring that every order approving surveillance direct "that the minimization procedures be followed.") Furthermore, the authorizing "judge may assess compliance with the minimization procedures" throughout the order's duration "by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated." 50 U.S.C. § 1805(d)(3); see United States v. Kashmiri, No. 09 CR 830-4, 2010 WL 4705159, at *5 (N.D. Ill. Nov. 10, 2010) (noting that FISA's allowance of "continuing oversight of the minimization procedures during the surveillance period" supports the constitutionality of the statute).

The Second Circuit has yet to decide "how the purpose for which a warrant is sought might inform the duty to minimize the interception of material not relevant to that purpose." Abu-Jihaad, 630 F.3d at 120 n.23; cf. Scott v. United States, 436 U.S. 128, 131 (1978) (affirming the requirement, in the context of criminal surveillance, of "an evaluation of the reasonableness of the actual interceptions in light of the purpose of the wiretap and the totality of the circumstances"). Nevertheless, courts routinely have upheld the legality of surveillance for which the government utilized the very minimization techniques defendant now challenges as per se unconstitutional. See, e.g., Abu-Jihaad, 630 F.3d at 120 n.23 (concluding that the FISA record before the panel "raise[d] no minimization concerns."); Rahman, 861 F.Supp. at 252 (upholding the propriety of "[t]he minimization procedures followed," which "were the standard

minimization procedures incorporated in the surveillance orders at issue"); United States v. Thomson, 752 F.Supp. 75, 80 (W.D.N.Y. 1990) ("[T]he Court finds that the government fully complied with all FISA minimization requirements.").

To the extent that defendant equates "open-ended" with overbroad, this Court similarly affirms that the minimization permitted by FISA is constitutional. FISA's "statutory scheme . . . to a large degree centers on an expanded conception of minimization that differs from that which governs law-enforcement surveillance." United States v. Belfield, 692 F.2d 141, 148 (D.C. Cir. 1982). In the latter context, "[i]nnocent parties are protected from unreasonable surveillance by the requirement . . . that surveillance 'shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception.'" United States v. Figueroa, 757 F.2d 466, 471 (2d Cir. 1985) (quoting Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), 18 U.S.C. § 2518(5)). Conversely, during the execution of FISA warrants, "surveillance devices are normally left on continuously, and the minimization occurs in the process of indexing and logging the pertinent communications.'"[7] Sattar, 2003 WL 22137012 at *10 (quoting In re Sealed Case, 310 F.3d at 740). Whereas Title III "requires minimization of what is acquired[,] . . . FISA requires minimization of what is acquired, retained, and disseminated." In re Sealed Case, 310 F.3d at 740; compare 18 U.S.C. § 2518(5) (requiring surveillance to be conducted "in such a way as to *minimize the interception* of communications not otherwise subject to interception" (emphasis added)); with 50 U.S.C. § 1801(h)(1) (requiring the adoption and implementation of procedures "reasonably designed in light of the purpose and technique of the particular surveillance, to *minimize the acquisition and*

[7] Again, "'[t]he reasonableness of this approach depends on the facts and circumstances of each case.'" Sattar, 2003 WL 22137012 at *10 (quoting In re Sealed Case, 310 F.3d at 740).

retention, and prohibit the dissemination, of nonpublicly available information" (emphasis added)).

Unlike traditional criminal surveillance, FISA monitoring does not have as its singular goal the gathering of evidence for the prevention or prosecution of "a particular offense." 18 U.S.C. § 2518(3)(a); see also 18 U.S.C. § 2516(1)(a)-(s) (listing offenses whose investigation will support issuance of a Title III warrant for electronic surveillance). Rather, it takes place "for the purpose of obtaining foreign intelligence information," 50 U.S.C. § 1802(b), which is defined in part as information that is "necessary to . . . the ability of the Unites States to protect against . . . actual or potential attack," 50 U.S.C. § 1801(e)(1)(A), or "necessary to . . . the national defense or the security of the United States," 50 U.S.C. § 1801(e)(2)(A). Such a purpose is broad by nature, as is the concept of necessity as that term is used within the statutory definition. To this end, the Congress that enacted FISA observed that "bits and pieces of information, which taken separately could not possibly be considered 'necessary,' may together or over time take on significance and become 'necessary.'"[8] H.R. Rep. No. 95–1283, pt. I, at 58-59 (1978) ("[A] lead which initially ends in a 'dry hole' can hardly be considered a dead issue, although it may be temporarily shelved to divert limited resources to other leads.").

Thus, as the Second Circuit has explained, differing standards of minimization "'may be compatible with the Fourth Amendment in light of the different purposes and practical considerations'" involved. Abu-Jihaad, 630 F.3d at 121-22 (quoting Duggan, 743 F.2d at 72). Indeed, minimization—whether before, during or after the fact—is an added layer of prophylaxis

[8] FISA's legislative history is rich with similar references to "minimizing" intercepts after they occur. See, e.g., S. Rep. No. 95-701, at 35 (1978) (Report of the Senate Select Committee on Intelligence) ("[W]here it cannot be determined immediately whether a certain piece of information is irrelevant, minimization procedures should require that within a specified time such a determination be made and the irrelevant matter expunged."); H.R. Rep. 95-1283, Pt. I, at 55 (1978) (Report of the House Permanent Select Committee on Intelligence) ("[I]n many cases it may not be possible for technical reasons to avoid acquiring all information. In these situations, the reasonable design of the procedures must emphasize the minimization of retention and dissemination.").

employed only when the surveillance targets a United States person.[9] See Duggan, 743 F.2d at 75-76. Given the government's compelling need to learn about the comings and goings of putative terrorists and counterintelligence agents, along with the difficulty of deciphering such information once acquired, contemporaneous minimization may well be a courtesy that is rarely afforded and not constitutionally mandated as long as FISA's other requirements are met. See, e.g., In re Terrorist Bombings of U.S. Embassies in E. Africa, 552 F.3d 157, 175-76 (2d Cir. 2008) (hereinafter "In re Terrorist Bombings II") (noting both that "foreign intelligence gathering . . . must delve into the superficially mundane because it is not always readily apparent what information is relevant" and that "members of covert terrorist organizations . . . often communicate in code, or at least in ambiguous language."). The government need not deprive itself of valuable security information by cutting off the acquisition of such information before its value becomes evident. Hence, when the government monitors citizens to obtain foreign intelligence information, FISA's minimization model successfully calibrates "the scope of the intrusion [against] the government's surveillance needs" for Fourth Amendment purposes. Id. at 175; see also Duggan, 743 F.2d at 73-74 (finding the minimization requirement, as defined, to be an ingredient of FISA's "constitutionally adequate balancing"); Belfield, 692 F.2d at 148 ("In FISA Congress has made a thoroughly reasonable attempt to balance the competing concerns of individual privacy and foreign intelligence.").

On a related note, defendant declares that "permitting the executive branch to define its own minimization procedures" violates the principle of separation of powers. Def. Br. at 6. This contention is without merit. As explained above, although FISA directs the Attorney General to promulgate minimization procedures, see 50 U.S.C. § 1801(h)(1), the resulting procedures must

[9] FISA defines a "United States person" to include U.S. citizens and aliens lawfully admitted for permanent residence. See 50 U.S.C. § 1801(i).

fit within the statutory definition enacted by Congress and their implementation requires the approval of an Article III court. In this regard, "the powers of all three branches of government—in short, the whole of federal authority—are invoked in determining when warrants may reasonably be sought and issued for the purpose of obtaining foreign intelligence information." Abu-Jihaad, 630 F.3d at 121. As the FISA review court[10] has suggested, an alternative approach, besides being inconsistent with the statute, may itself run afoul of the Constitution. See In re Sealed Case, 310 F.3d at 731 (suggesting that by adopting and then imposing its own minimization procedures, "the FISA Court may well have exceeded the constitutional bounds that restrict an Article III court" because "the Attorney General has the responsibility to determine how to deploy personnel resources").

4. Executive Branch "Findings"

Fourth, defendant argues that FISA violates separation of powers by permitting the executive branch to make its own probable cause determinations regarding whether the proposed target of surveillance is engaging in criminal activity. Def. Br. at 5. Such an assertion misapprehends FISA in several key respects.

First, no branch of government—whether executive or judicial—need make a probable cause finding of *actual or potential criminal activity* to justify a FISA warrant. Indeed, as discussed previously, FISA authorizes applications for electronic and other surveillance "'for the purpose of obtaining foreign intelligence information.'" Abu-Jihaad, 630 F.3d at 117 (quoting 50 U.S.C. § 1802(b)). Although "multiple purposes may be inevitable given FISA's definition of 'foreign intelligence information' and 'agent of a foreign power' by reference to serious criminal conduct," id. at 127, "otherwise valid FISA surveillance is not tainted simply because the

[10] See 50 U.S.C. § 1803(b) ("The Chief Justice shall publicly designate three judges . . . from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this chapter.").

government can anticipate that the fruits of such surveillance may later be used, as allowed by [FISA], as evidence in a criminal trial," Duggan, 743 F.2d at 78. Accordingly, the governmental concerns prompting FISA's enactment "make reasonable the adoption of prerequisites to surveillance that are less stringent than those precedent to the issuance of a warrant for a criminal investigation." Id. at 73. The FISA Court need not find that probable cause exists to believe that surveillance will in fact produce the sought-after intelligence. By extension, the executive certainly need not illustrate, unilaterally or otherwise, "probable cause to believe the target has committed a crime." Id. at 73 n.5.

Moreover, the FISA Court makes the required probable cause determination, and in doing so, reviews "the facts submitted by the [executive branch] applicant," 50 U.S.C. § 1805(a)(2), and "may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target," 50 U.S.C. § 1805(b). The executive branch facilitates that process by including, in every application for surveillance, "a statement of the facts and circumstances relied upon by the applicant to justify his belief" that the statute's probable cause requirements are met. 50 U.S.C. § 1804(a)(3).

To the extent defendant's argument may be construed to mean that the judicial branch does not review FISA applications in depth, such a result is by design. "FISA warrant applications are subject to 'minimal scrutiny by the courts,' both upon initial presentation and subsequent challenge." Abu-Jihaad, 630 F.3d at 130 (quoting Duggan, 743 F.2d at 77). For example, "the representations and certifications submitted in support of an application for FISA surveillance should be presumed valid by a reviewing court absent a showing sufficient to trigger a Franks hearing." Id. at 130 (citing Franks v. Delaware, 438 U.S. 154 (1978)) (internal quotation marks omitted). Likewise, "'[a] reviewing court [has] no greater authority to second-

guess the executive branch's certifications than has the FISA Judge.'" Stewart, 590 F.3d at 128 (quoting Duggan, 743 F.2d at 77).

Deferential review, however, does not mean that such review is superficial. See Abu-Jihaad, 630 F.3d at 130 ("Of course, even minimal scrutiny is not toothless."). This Court, for example, has thoroughly reviewed the government's submissions to confirm that FISA's procedural and substantive requirements have been met in this case. The Court will not endorse the suggestion that other federal courts routinely "shirk [their] responsibilities to protect the constitutional rights of all citizens," Simmons v. Reynolds, 898 F.2d 865, 870 (2d Cir. 1990), including those whom the government elects for presumably legitimate reasons to surveil. Although the FISA Court's "finding of probable cause is itself a substantial factor tending to uphold the validity of [a] warrant," as the Second Circuit has held in the case of criminal search warrants, "it remains for the reviewing court to decide whether the [FISA judge] performed his neutral and detached function on the facts before him." United States v. Travisano, 724 F.2d 341, 345 (2d Cir. 1983). Thus, FISA's probable cause requirement does not commit to the executive, either de jure or de facto, a function, which properly inheres to the courts.

5. Definition of "Agent of a Foreign Power"

Fifth, defendant argues that FISA's definition of "agent of a foreign power" is impermissibly broad because it includes persons whose activities "may" violate federal law. Def. Br. at 6. It is unclear whether defendant argues that the statute's probable cause requirements are unconstitutionally lax—a proposition rejected repeatedly by the Second Circuit, see discussion and cases cited, supra Part I.A. & I.A.1—or that the definition of "agent of a foreign power" encompasses individuals who are not justifiable targets of foreign intelligence monitoring—a proposition rejected by the Second Circuit only once, albeit soundly. See

Duggan, 743 F.2d at 71 ("We find no merit in the[] contention[]" that FISA's definition of "agent of a foreign power" renders the statute "impermissibly broad.") The latter argument is based on the definition appearing in 50 U.S.C. § 1801(b)(2)(A), relating to persons who "knowingly engage[] in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or *may involve* a violation of the criminal statutes of the United States." Id. (emphasis added). The inference, unstated in defendant's moving papers, would be that such a definition potentially makes anyone the "agent of a foreign power."

"Interesting though these arguments may be in the abstract, they have no application to the case at hand," Duggan, at 71, for Medujanin's alleged conduct fits within the alternative definitions of "agent of a foreign power" contained 50 U.S.C. §§ 1801(b)(2)(C) and 1801(b)(2)(E). These provisions cover any individual who "knowingly engages in sabotage or international terrorism, or *activities that are in preparation therefor*," 50 U.S.C. § 1801(b)(2)(C) (emphasis added), or who "knowingly aids or abets" or "knowingly conspires with any person to engage in [those] activities," on behalf of a foreign power, 50 U.S.C. § 1801(b)(2)(E). In this case, that "foreign power" would be al-Qaeda, "a group engaged in international terrorism." 50 U.S.C. § 1801(a)(4). Therefore, "[t]he sections and definitions plainly applicable to [defendant] are explicit, unequivocal, and clearly defined," Duggan, 743 F.2d at 71, and "[t]he sections of the Act relied upon by [defendant] to show that the Act is impermissibly broad are simply irrelevant to this case." Id.

B. Disclosure of the FISA Dockets

Defendant seeks an order compelling disclosure of the FISA applications and orders on two related grounds. First, defendant seeks to inspect the dockets "to determine whether grounds exist to move to suppress the FISA evidence," Def. Br. at 7, by implication challenging this

Court's ex parte, in camera review of the documents. Second, defendant argues that "absent disclosure," defense counsel "will not be able to perform their constitutionally dictated function of providing effective representation." Id. As discussed below, neither contention justifies unsealing the FISA dockets in this case.

1. Proceeding Ex Parte *and* In Camera

"FISA applications are likely to contain allegedly sensitive information relating to perceived issues of national security." Stewart, 590 F.3d at 128. Hence, "disclosure of FISA materials 'is the exception and ex parte, in camera determination is the rule.'" Abu-Jihaad, 630 F.3d at 129 (quoting Stewart, 590 F.3d at 129). Contrary to defendant's assertion, the presumption of ex parte review—which is made explicit in FISA's text—does not impinge upon defendant's Fifth Amendment guarantee of Due Process or Sixth Amendment right to adequate representation, either in the abstract or under the circumstances.

It is true that a court must unseal the FISA applications and orders "'to the extent that due process requires discovery or disclosure.'" Abu-Jihaad, 630 F.3d at 129 (quoting 50 U.S.C. § 1806(g)). But to hold that the Constitution always requires disclosure of the underlying materials would frustrate the clearly expressed policy choices of the legislative and executive branches regarding national security. Rather, "the decision whether to allow a defendant to obtain FISA materials is made by a district judge on a case by case basis," as is the finding "whether such a decision protects a defendant's constitutional rights." In re Sealed Case, 310 F.3d at 741 n.24.

"In FISA, Congress expressly provided that where, as here, the Attorney General certifies that 'disclosure [of FISA materials] or an adversary hearing would harm the national security of the United States,' a district court must 'review in camera and ex parte the application, order, and

such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.'" Abu-Jihaad, 630 F.3d at 129 (quoting 50 U.S.C. § 1806(f)). The Attorney General submits the contemplated certification, which mirrors the statutory language and incorporates a classified declaration describing the basis for the government's belief that disclosing the FISA dockets to the defense would harm national security. See Gov't Br., Exs. 1-2. Accordingly, this Court "shall" review the relevant applications and orders in camera and ex parte "notwithstanding any other law." 50 U.S.C. § 1806(f).

The Second Circuit has made clear that proceeding ex parte does not, standing alone, offend notions of fundamental fairness. See, e.g., Abu-Jihaad, 630 F.3d at 129 (finding "no denial of due process in the district court's decision not to order disclosure of FISA materials to the defendant, or to conduct a preliminary hearing to rule on [the defendant]'s challenge to FISA's implementation"); Stewart, 590 F.3d at 129 (finding "no error in the district court's determination that disclosure was unnecessary for an accurate determination of the legality of the surveillance at issue or to satisfy the requirements of due process."); Duggan, 743 F.3d at 78 ("Defendant's contention that the district court erred in refusing to disclose the substance of the affidavits and certifications that accompanied the FISA applications need not detain us long."); see also United States v. Ott, 827 F.2d 473, 475 (9th Cir. 1987) (affirming the district court's rejection of the defendant's "claim that FISA's provision for ex parte, in camera review of the surveillance materials violated his fifth and sixth amendment rights"); United States v. Benkahla, 437 F.Supp.2d 541, 554 (E.D. Va. 2006) (rejecting the notion that "in camera, ex parte review of FISA materials" violates a defendant's "Fifth Amendment right to due process and his Sixth Amendment right to counsel").

Moreover, "[t]here would be little purpose in disclosure unless [defense counsel] were then allowed to present their case against the legality of the surveillance." Belfield, 692 F.2d at 147. In this case, however, an adversary hearing would be academic because there is no question the FISA applications pass muster. Indeed, "'accurate resolution of the factual issues would not have been materially advanced by either disclosure of the information to the defendant or an adversary hearing.'" In re Terrorist Bombings II, 552 F.3d at 165 (quoting United States v. Ajlouny, 629 F.2d 830, 839 (2d Cir.1980)); see also Belfield, 692 F.2d at 147 (affirming that the "decision to pass upon the legality of the surveillance based upon an ex parte examination of an in camera" submission "[i]s in keeping with the procedures contemplated by Congress when it enacted FISA."). Having reviewed the classified, but otherwise unremarkable, FISA dockets in their entirety, the Court readily concludes that possession of these materials is of no benefit to any defense that could be mounted.

Defense counsel's security clearances add little to the case for disclosure. "'Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to anyone not involved in the surveillance operation in question, whether or not she happens for unrelated reasons to enjoy security clearance.'" United States v. Bin Laden, 126 F.Supp.2d 264, 287 n. 27 (S.D.N.Y. 2000) (quoting Ott, 827 F.2d at 477); accord United States v. Libby, 429 F.Supp.2d 18, 24 n. 8 (D.D.C. 2006) ("It is axiomatic that even if the defendant and his attorneys had been granted the highest level of security clearances, that fact alone would not entitle them to access to [(sic)] every piece of classified information this country possesses."). As the government persuasively argues, unsealing the FISA materials in this case would provide the defense with unnecessary details of an extraordinarily sensitive anti-terrorism investigation.

Neither the Fifth nor the Sixth Amendment affords the defense such access to this information. Information contained in the FISA applications "would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods." United States v. Yunis, 867 F.2d 617, 625 (D.C. Cir. 1989) (holding disclosure of classified information unwarranted where it is "not helpful to the presentation of the defense or essential to the fair resolution of the cause"); see also In re Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 93, 117 n.22 (2d Cir. 2008) ("Al-Qaeda members submit 'security reports' to al Qaeda's headquarters [regarding] . . . the efforts of Western intelligence and law enforcement agencies to arrest or capture al Qaeda members.").

2. Legality of Surveillance

Alternatively, defendant seeks to inspect the FISA applications and orders to determine whether valid arguments for suppression exist. The statute allows disclosure of the FISA dockets "under appropriate security procedures and protective orders" in the limited circumstance "where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C § 1806(f). Such a need might arise if in camera review reveals, for example, "'potential irregularities such as possible misrepresentation of fact, vague identification of the persons to be surveilled or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order.'" Stewart, 590 F.3d at 129 (quoting Duggan, 743 F.2d at 78 (internal quotation marks and brackets omitted)). Notwithstanding this small measure of discretion, "[n]o United States District Court or Court of Appeals has ever determined that disclosure to the defense of such materials was necessary to determine the lawfulness of surveillance or searches under FISA." United States v. Warsame, 547 F.Supp.2d

982, 987 (D. Minn. 2008). Defendant "does not point to any case where any court has ordered disclosure in a situation similar to" his. Stewart, 590 F.3d at 129.

The Court recognizes the difficulty defense counsel faces in blindly arguing "that the determination of legality is so complex that an adversary hearing with full access to relevant materials is necessary." Belfield, 692 F.2d at 147-48 (comparing the task to "punching at shadows"). Defense counsel, however, may not inspect the FISA dockets to construct a better argument for inspecting the FISA dockets. Such a circular exercise would be patently inconsistent with FISA and unjustified by the facts presented. See United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987) (rejecting the defendant's request for "disclosure of the FISA application, ostensibly so that he may review it for errors").

To the extent defense counsel's request may be construed as challenging whether FISA's requirements were met, the Court affirms, based upon the record before it, that the surveillance at issue was conducted in conformity with FISA. "Although the established standard of judicial review applicable to FISA warrants is deferential, the government's detailed and complete submissions in this case would easily allow it to clear a higher standard of review." Abu-Jihaad, 630 F.3d at 129-30 (finding disclosure not required where the FISA materials were "relatively straightforward and not complex" and "in camera, ex parte review permitted [the panel] to assess the legality of the challenged surveillance") (internal quotation marks omitted); Warsame, 547 F.Supp.2d at 987 (finding disclosure not required where "the issues presented by the FISA applications [we]re straightforward and uncontroversial, and present[ed] none of the concerns that might warrant disclosure"); Thomson, 752 F.Supp. at 79 ("[T]he issues in this case are not so complex that the participation of the defendant is required to accurately determine the legality of the surveillance at issue."). The FISA applications in this case more than adequately satisfy

the requirements set forth in 50 U.S.C. § 1804 and do so with clarity and specificity. The Court cannot say more without the risk of divulging classified information. Furthermore, nothing in the applications "provides any basis to think that the FISA application contained any false statement, much less one made 'knowingly and intentionally, or with reckless disregard for the truth.'" Abu-Jihaad, at 131 (quoting Franks v. Delaware, 438 U.S. 154, 155 (1978)).

Additionally, the Court is satisfied that the minimization techniques utilized by the government were "reasonably designed in light of the purpose and technique of the particular surveillance" involved. 50 U.S.C. § 1801(h)(1). The Supreme Court has outlined a number of factors that militate toward allowing increased leeway to government surveillance. For example, communications may be "ambiguous in nature or apparently involve[] guarded or coded language," Scott, 436 U.S. at 140; when a conspiracy is thought to be widespread, "more extensive surveillance may be justified in an attempt to determine the precise scope of the enterprise," id.; and "[d]uring the early stages of surveillance the agents may be forced to intercept all calls to establish categories of nonpertinent calls which will not be intercepted thereafter," id. at 141. Each of these factors counsels for a lenient approach to minimization in the present case. Thus, the proposed minimization procedures unquestionably met or exceeded the minimum allowable safeguards. On a more fundamental level, any "intrusion on [defendant]'s privacy was outweighed by the government's manifest need to monitor his activities as [a potential] operative of al Qaeda because of the extreme threat al Qaeda presented, and continues to present, to national security." In re Terrorist Bombings II, 552 F.3d at 172-73.

The Court also is satisfied that "minimization procedures [were] followed" in this case. 50 U.S.C. § 1805(c)(2)(A). The government notes that it inadvertently failed to follow accepted minimization procedures relating to the handling of a small subset of intercepted

communications. See Gov't Submission 118-22 & Exhibit 3. These few intercepts were "not made in conformity with an order of authorization or approval." 50 U.S.C. § 1806(e)(2). In a classified letter dated May 23, 2011, however, the government more fully explains the steps it took to remedy the inadequacies and the nature of the intercepted communications. Based on the government's submissions, the Court concludes that any failure to adhere to protocol was de minimis, that the consequences were equally negligible, and that "'on the whole the agents have shown a high regard for the right of privacy and have done all they reasonably could to avoid unnecessary intrusion.'" S. Rep. No. 95-701, at 39-40 (quoting United States v. Tortorello, 480 F.2d 764, 784 (2d Cir. 1973). Thus, the Court will not suppress the surveillance on this basis.

II. CONCLUSION

For the reasons stated above, the Court reaffirms that FISA is facially constitutional, that its requirements were met in this case, and that defendant has not made the requisite showing to warrant discovery of the FISA applications and orders. Therefore, defendant's motion to suppress evidence obtained by the government pursuant to FISA is DENIED.

SO ORDERED.

Dated: Brooklyn, New York
February 16, 2012

s/ Judge Raymond J. Dearie

RAYMOND J. DEARIE
United States District Judge